AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of establishing a wireless connection between a first device and ~~to~~ a second device, said method comprising:

displaying at said first device a list of available devices within wireless range of said first device, said list including said second device;

receiving at said first device a selection of said second ~~a~~ device from ~~that is included~~ in said list;

connecting wirelessly with said second device;

exchanging passkeys with said second device, said exchanging comprising sending a first passkey from said first device to said second device and receiving at said first device a second passkey from said second device;

storing said second passkey in memory at said first device;

receiving at said first device a user input that selects a designation for said second device, wherein ~~designating said device as~~ said designation identifies said second device as either a trusted device or a non-trusted device, wherein if said second device is designated as a trusted device then said second passkey is automatically used for subsequent connections with said second device and [[,]] wherein said second passkey is retrieved from said memory such that ~~and wherein~~ manual input of said second passkey is obviated for said subsequent connections, and if said second device is designated as a non-trusted device then said second passkey is not automatically used and wherein further a connection with said second device is permitted without passkeys, wherein a level of security for a connection with said second device depends on whether said second device is designated as a trusted device or as a non-trusted device; and

indicating said designation for ~~that~~ said second device ~~is a trusted device~~ in said list, wherein said list includes trusted devices and non-trusted devices and wherein in said list said trusted devices are distinguished from said non-trusted devices [[,]] ~~wherein further a connection with a non-trusted device in said list is permitted without passkeys, wherein a level of security for a connection with any device selected from said list depends on whether said any device is designated a trusted device or a non-trusted device~~.

2. (Previously Presented) The method as recited in Claim 1 wherein said connecting is performed substantially according to BLUETOOTH protocols.

3-6. (Canceled).

7. (Previously Presented) The method as recited in Claim 1 comprising:

deleting a device from said list.

8. (Previously Presented) The method as recited in Claim 1 wherein said second passkey is valid only for a specified period of time.

9. (Currently Amended) A system comprising:

a display device;

a transceiver coupled to said display device;

a processor coupled to said display device; and

a memory coupled to said display device, said memory containing instructions that when executed implement a method of establishing a wireless connection to a second ~~another~~ device, said method comprising:

receiving into said system a passkey from said second device during a first connection with said second device;

receiving into said system a user input indicating that said second device is being designated a trusted device, wherein as a trusted device said passkey is to be automatically used for subsequent connections with said second device;

as a result of receiving said user input indicating that said device is being designated a trusted device, associating said passkey with said second device in said memory and ending said first connection;

receiving at said system a user input selecting said second device for a second connection subsequent to said first connection;

connecting said system wirelessly with said second device;

determining a level of security associated with said second connection;

if required by said level of security, making said second connection by automatically retrieving and using said passkey for said second device from said memory, wherein manual input of said passkey is obviated for said second connection and, if not required by said level of security, making said second connection without said passkey;

displaying on said display device a list of devices within wireless range of said system; and

indicating that said second device is a trusted device in said list, wherein said list includes trusted devices and non-trusted devices and wherein in said list said trusted devices are distinguished from said non-trusted devices.

10. (Previously Presented) The system of Claim 9 wherein said connecting of said method is performed substantially according to BLUETOOTH protocols.

11-14. (Canceled).

15. (Previously Presented) The system of Claim 9 wherein said method comprises:

deleting a device from said list.

16. (Original) The system of Claim 9 wherein said passkey is valid only for a specified period of time.

17. (Currently Amended) A computer-usable medium having computer-readable code stored thereon for causing a first device to perform a method of establishing a wireless connection to a second ~~another~~ device, said method comprising:

displaying at said first device a list of available devices within wireless range of said first device, said list including said second device;

receiving at said first device a selection of said second ~~another~~ device from ~~that is included~~ in said list;

connecting wirelessly with said second ~~other~~ device;

exchanging passkeys with said second ~~other~~ device, said exchanging comprising sending a first passkey from said first device to said second ~~other~~ device and receiving at said first device a second passkey from said second ~~other~~ device;

receiving at said first device a user input indicating that selects a designation for said second ~~other~~ device, wherein said designation identifies said second device as either ~~is being designated~~ a trusted device or a non-trusted device, wherein if said second device is designated as a trusted device then said first and second passkeys are ~~to be~~ automatically used for subsequent connections with said second ~~other~~ device;

as a result of receiving said user input indicating that said other device is being designated a trusted device, storing said second passkey in memory at said first device, wherein if said second device is designated as a trusted device then said first and second passkeys are automatically retrieved from said memory and used for said subsequent connections such that manual input of said first and second passkeys is obviated for said subsequent connections, and if said second device is designated as a non-trusted device then said second passkey is not automatically used and wherein further a connection with said second device is permitted without said first and second passkeys, wherein a level of security for a connection with said second device depends on whether said second device is designated as a trusted device or as a non-trusted device;

~~automatically using said first and second passkeys for subsequent connections with said other device, wherein said first and second passkeys are retrieved from memory and wherein manual input of said first and second passkeys is obviated for said subsequent connections;~~ and

indicating said designation for ~~that~~ said second ~~other~~ device ~~is a trusted device~~ in said list, wherein said list includes trusted devices and non-trusted devices and wherein in said list said trusted devices are distinguished from said non-trusted devices [[,]] ~~wherein further a connection with a non-trusted device in said list is permitted without passkeys, wherein a level of security for a~~

~~connection with a non-trusted device is reduced relative to a connection with a trusted device in said list~~.

18. (Previously Presented) The computer-usable medium of Claim 17 wherein said connecting are performed substantially according to BLUETOOTH protocols.

19-22. (Canceled).

23. (Currently Amended) The computer-usable medium of Claim 17 wherein said computer-readable program code embodied therein causes said first device to perform said method comprising:

deleting a device from said list.

24. (Previously Presented) The computer-usable medium of Claim 17 wherein said second passkey is valid only for a specified period of time.

25. (Currently Amended) The method of Claim 1 comprising:

placing an icon adjacent the name of said second device in said list to indicate that said second device is a trusted device.

26. (Currently Amended) The computer-usable medium of Claim 17 wherein said computer-readable program code embodied therein causes said first device to perform said method comprising:

placing an icon adjacent the name of said second ~~other~~ device in said list to indicate that said second ~~other~~ device is a trusted device.